OPS.3.2.A19 Sicherheitsüberprüfung von Beschäftigten (H)

Die Vertrauenswürdigkeit des Personals der Anbietenden von Outsourcing SOLLTE durch geeignete Nachweise überprüft werden. Es SOLLTEN mit den Nutzenden von Outsourcing vertragliche Kriterien vereinbart werden.

OPS.3.2.A20 Verschlüsselte Datenübertragung und -speicherung (H)

Für die Übertragung von Daten von und zu den Nutzenden von Outsourcing sowie die Speicherung SOLLTE mit den Nutzenden von Outsourcing eine sicheres Verschlüsselungsverfahren festgelegt werden. Dabei SOLLTE sich die eingesetzte Verschlüsselungsmethode am Schutzbedarf der Daten orientieren. Die Verschlüsselungsmethode SOLLTE regelmäßig und anlassbezogen auf ihre Funktionsfähigkeit hin überprüft werden.

OPS.3.2.A21 Durchführung von gemeinsamen Notfall- und Krisenübungen (H) [Notfallbeauftragte]

Gemeinsame Notfall- und Krisenübungen mit den Nutzenden von Outsourcing SOLLTEN durchgeführt und dokumentiert werden (siehe DER.4 *Notfallmanagement*). Das Resultat der Übung SOLLTE dazu genutzt werden, um das Notfallkonzept sowie insbesondere die gemeinsamen Maßnahmenpläne zu verbessern. Die Notfall- und Krisenübungen SOLLTEN regelmäßig und anlassbezogen durchgeführt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Kapitel A.15.2 „Steuerung der Dienstleistungserbringung von Lieferanten" Vorgaben für die Steuerung von Dienstleistenden. In der DIN ISO 37500:2015-08 werden im „Leitfaden Outsourcing" weiterführende Informationen zum Umgang mit Dienstleistenden aufgeführt.

Des Weiteren wird in der ISO 27002:2021 das Outsourcing-Verhältnis von Kapitel 5.19 bis 5.22 detailliert aufgeführt und spezifiziert somit die Vorgaben der ISO/IEC 27001:2013.

Der „Leitfaden zur Umsetzung rechtlicher Rahmenbedingungen" des Bundesverbandes Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom) führt Informationen zur Thematik „Compliance" in IT-Outsourcing-Projekten auf und liefert Hilfestellungen zur Umsetzung der rechtlichen Rahmenbedingungen in einem Outsourcing-Verhältnis.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-53 Anforderungen an Dienstleistende. In einer weiteren Publikation NISTIR 8276 beschreibt NIST die Best-Practices im Risikomanagement einer „Cyber Supply Chain".

Der BSI-Standard 200-4 Notfallmanagement enthält wichtige Informationen sowie Vorlagen zur Erstellung und Etablierung eines funktionsfähigen Notfallkonzepts.

DER: Detektion und Reaktion

Bundesamt
für Sicherheit in der
Informationstechnik

DER.1 Detektion von sicherheitsrelevanten Ereignissen

1. Beschreibung

1.1. Einleitung

Um IT-Systeme schützen zu können, müssen sicherheitsrelevante Ereignisse rechtzeitig erkannt und behandelt werden. Dazu ist es notwendig, dass Institutionen im Vorfeld geeignete organisatorische, personelle und technische Maßnahmen planen, implementieren und regelmäßig üben. Denn wenn auf ein vorgegebenes und erprobtes Verfahren aufgesetzt werden kann, lassen sich Reaktionszeiten verkürzen und vorhandene Prozesse optimieren.

Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, das sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen kann. Typische Folgen solcher Ereignisse sind ausgespähte, manipulierte oder zerstörte Informationen. Die Ursachen dafür sind dabei vielfältig. So spielen unter anderem Malware, veraltete IT-Systeminfrastrukturen oder Innentäter und Innentäterinnen eine Rolle. Angreifende nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, bevor es für diese einen Patch gibt. Eine weitere ernstzunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APTs). Dabei handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich Angreifende dauerhaften Zugriff zu einem Netz verschaffen und diesen Zugriff in der Folge auf weitere IT-Systeme ausweiten. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifenden aus und sind oft schwer zu detektieren.

1.2. Zielsetzung

Dieser Baustein zeigt einen systematischen Weg auf, wie Informationen gesammelt, korreliert und ausgewertet werden können, um sicherheitsrelevante Ereignisse möglichst vollständig und zeitnah zu detektieren. Die aus der Detektion gewonnenen Erkenntnisse sollen die Fähigkeit von Institutionen verbessern, sicherheitsrelevante Ereignisse zu erkennen und angemessen darauf zu reagieren.

1.3. Abgrenzung und Modellierung

Der Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* ist auf den Informationsverbund einmal anzuwenden.

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn sicherheitsrelevante Ereignisse detektiert werden sollen. Voraussetzung hierfür ist jedoch, dass umfassend protokolliert wird. Die dafür notwendigen Anforderungen werden nicht im vorliegenden Baustein beschrieben, sondern sind im Baustein OPS.1.1.5 *Protokollierung* enthalten.

Im Vorfeld der Detektion von sicherheitsrelevanten Ereignissen ist es wichtig, dass Zuständigkeiten und Kompetenzen klar definiert und zugewiesen werden. Es sollte insbesondere auf den Grundsatz der Funktionstrennung geachtet werden. Dieses Thema ist nicht Bestandteil dieses Bausteins, sondern wird im Baustein ORP.1 *Organisation* behandelt.

Außerdem beschreibt der Baustein nicht, wie mit sicherheitsrelevanten Ereignissen umzugehen ist, nachdem sie detektiert worden sind. Anforderungen dazu werden in den Bausteinen DER.2.1 *Behandlung von Sicherheitsvorfällen* und DER.2.2 *Vorsorge für die IT-Forensik* aufgeführt. Ebenso wird nicht auf das Thema Datenschutz eingegangen, dieses wird im Baustein CON.2 *Datenschutz* behandelt.

Um sicherheitsrelevante Ereignisse zu erkennen, sind oft zusätzliche Programme erforderlich, z. B. Antivirenprogramme, Firewalls oder Intrusion Detection /Intrusion Prevention Systeme (IDS/IPS). Sicherheitsaspekte dieser Systeme sind ebenfalls nicht Gegenstand des vorliegenden Bausteins. Sie werden z. B. in den Bausteinen OPS.1.1.4 *Schutz vor Schadprogrammen* bzw. NET.3.2 *Firewall* thematisiert.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* von besonderer Bedeutung.

2.1. Missachtung von gesetzlichen Vorschriften und betrieblichen Mitbestimmungsrechten

Programme, die sicherheitsrelevante Ereignisse detektieren und Protokolldaten auswerten, sammeln oft viele Informationen über die Netzstruktur und die internen Abläufe einer Institution. Darin können schützenswerte Informationen wie personenbezogene Daten, vertrauliche Daten oder Arbeitsabläufe von Mitarbeitenden enthalten sein. Dadurch, dass solche Daten gespeichert werden, können jedoch Persönlichkeitsrechte bzw. Mitbestimmungsrechte verletzt werden. Auch verstößt die Institution unter bestimmten Voraussetzungen eventuell gegen die jeweiligen Datenschutzgesetze.

2.2. Unzureichende Qualifikation der Mitarbeitenden

Im täglichen IT-Betrieb einer Institution können viele Störungen und Fehler auftreten, z. B. könnten ankommende Protokolldaten plötzlich stark zunehmen. Sind die Zuständigen nicht ausreichend sensibilisiert und geschult, kann es passieren, dass sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so Angriffe unerkannt bleiben. Und auch wenn die Zuständigen ausreichend für die Belange der Informationssicherheit sensibilisiert und geschult sind, kann trotzdem nicht ausgeschlossen werden, dass sie Sicherheitsvorfälle nicht erkennen. Beispiele dafür sind:

- Eine Person, die seit längerer Zeit nicht im lokalen Netz ihrer Institution angemeldet war, stuft es als normal ein, dass ihr Notebook seit einer Woche während des Internetzugangs deutlich langsamer ist. Sie bemerkt nicht, dass ein Schadprogramm im Hintergrund aktiv ist. Sie wurde nicht oder nur unzureichend geschult, bei verdächtigen Auffälligkeiten das Incident Management zu informieren.
- Eine Produktionsleitung bemerkt nicht, dass die Daten in den Produktionssystemen und auch die Steuerungsanzeigesysteme heimlich verändert wurden. Sie schöpft keinen Verdacht, als die SCADA-Steuerung der Produktionsanlage seltsame Werte anzeigt, da dies nur kurzzeitig erfolgte. Der Vorfall wird nicht gemeldet, da alle Werte wieder den erwarteten Anzeigewerten entsprechen. Dass eine Schadsoftware die Anzeigewerte manipuliert hat, fällt somit niemandem auf.

2.3. Fehlerhafte Administration der eingesetzten Detektionssysteme

Fehlerhafte Konfigurationen können dazu führen, dass eingesetzte Detektionssysteme nicht ordnungsgemäß funktionieren. Ist beispielsweise die Alarmierung falsch eingestellt, können vermehrt Fehlalarme auftreten. Die Zuständigen können dann eventuell nicht mehr zwischen einem Fehlalarm und einem sicherheitsrelevanten Ereignis unterscheiden. Auch nehmen sie die Meldungen möglicherweise nicht schnell genug wahr, da zu viele Alarme generiert werden. Dadurch bleiben möglicherweise Angriffe unerkannt. Ebenso steigt der Aufwand stark an, um die Menge der Meldungen auszuwerten.

2.4. Fehlende Informationen über den zu schützenden Informationsverbund

Sind keine oder nur ungenügende Informationen über den zu schützenden Informationsverbund vorhanden, kann es passieren, dass wesentliche Bereiche des Informationsverbunds nicht ausreichend durch Detektionssysteme abgesichert werden. Dadurch können Angreifende leicht in das Netz der Institution eindringen und z. B. schützenswerte Informationen abgreifen. Auch ist es ihnen so möglich, lange unbemerkt im System zu bleiben und dauerhaft auf das Netz zuzugreifen.

2.5. Unzureichende Nutzung von Detektionssystemen

Wenn keine Detektionssysteme eingesetzt werden und auch die in IT-Systemen und Anwendungen vorhandenen Funktionen zur Detektion von sicherheitsrelevanten Ereignissen nicht benutzt werden, können Angreifende leichter unbemerkt in das Netz der Institution eindringen. Dort könnten sie unbefugt auf sensible Informationen zugreifen. Besonders kritisch ist es, wenn die Übergänge zwischen Netzgrenzen nur unzureichend überwacht werden.

2.6. Unzureichende personelle Ressourcen

Ist nicht genügend Personal vorhanden, um Protokolldaten auszuwerten, können sicherheitsrelevante Ereignisse nicht vollständig detektiert werden. So bleiben Angriffe eventuell lange verborgen oder werden erst entdeckt, nachdem z. B. schon sehr viele schützenswerte Informationen abgeflossen sind. Auch wenn durch zu wenig Personal keine externen Informationsquellen ausgewertet werden, bleiben Sicherheitslücken eventuell zu lange offen. Dann können sie ausgenutzt werden, um unerlaubt in die IT-Systeme der Institution einzudringen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.1 *Detektion von sicherheitsrelevanten Ereignissen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Mitarbeitende, Fachverantwortliche, Benutzende, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen erstellt werden. In der spezifischen Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie die Detektion von sicherheitsrelevanten Ereignissen geplant, aufgebaut und sicher betrieben werden kann. Die spezifische Sicherheitsrichtlinie MUSS allen im Bereich Detektion zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein. Falls die spezifische Sicherheitsrichtlinie verändert wird oder von den Anforderungen abgewichen wird, dann MUSS dies mit dem oder der verantwortlichen ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung MÜSSEN sinnvoll dokumentiert werden.

DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten (B)

Wenn Protokollierungsdaten ausgewertet werden, dann MÜSSEN dabei die Bestimmungen aus den aktuellen Gesetzen zum Bundes- und Landesdatenschutz eingehalten werden. Wenn Detektionssysteme eingesetzt werden, dann MÜSSEN die Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitendenvertretungen gewahrt werden. Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden, z. B. das Telemediengesetz (TMG), das Betriebsverfassungsgesetz und das Telekommunikationsgesetz.

DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse (B)

Für sicherheitsrelevante Ereignisse MÜSSEN geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden. Es MUSS bestimmt werden, welche Stellen wann zu informieren sind. Es MUSS aufgeführt sein, wie die jeweiligen Personen erreicht werden können. Je nach Dringlichkeit MUSS ein sicherheitsrelevantes Ereignis über verschiedene Kommunikationswege gemeldet werden.

Alle Personen, die für die Meldung bzw. Alarmierung relevant sind, MÜSSEN über ihre Aufgaben informiert sein. Alle Schritte des Melde- und Alarmierungsprozesses MÜSSEN ausführlich beschrieben sein. Die eingerichteten Melde- und Alarmierungswege SOLLTEN regelmäßig geprüft, erprobt und aktualisiert werden, falls erforderlich.

DER.1.A4 Sensibilisierung der Mitarbeitenden (B) [Vorgesetzte, Benutzende, Mitarbeitende]

Alle Benutzenden MÜSSEN dahingehend sensibilisiert werden, dass sie Ereignismeldungen ihrer Clients nicht einfach ignorieren oder schließen. Sie MÜSSEN die Meldungen entsprechend der Alarmierungswege an das verantwortliche Incident Management weitergeben (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Alle Mitarbeitenden MÜSSEN einen von ihnen erkannten Sicherheitsvorfall unverzüglich dem Incident Management melden.

DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion (B) [Fachverantwortliche]

Falls eingesetzte IT-Systeme oder Anwendungen über Funktionen verfügen, mit denen sich sicherheitsrelevante Ereignisse detektieren lassen, dann MÜSSEN diese aktiviert und benutzt werden. Falls ein sicherheitsrelevanter Vorfall vorliegt, dann MÜSSEN die Meldungen der betroffenen IT-Systeme ausgewertet werden. Zusätzlich MÜSSEN die protokollierten Ereignisse anderer IT-Systeme überprüft werden. Auch SOLLTEN die gesammelten Meldungen in verbindlich festgelegten Zeiträumen stichpunktartig kontrolliert werden.

Es MUSS geprüft werden, ob zusätzliche Schadcodescanner auf zentralen IT-Systemen installiert werden sollen. Falls zusätzliche Schadcodescanner eingesetzt werden, dann MÜSSEN diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten. Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden. Die Zuständigen MÜSSEN die Meldungen auswerten und untersuchen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten (S)

Alle Protokollierungsdaten SOLLTEN möglichst permanent aktiv überwacht und ausgewertet werden. Es SOLLTEN Mitarbeitende benannt werden, die dafür zuständig sind.

Falls die zuständigen Mitarbeitenden aktiv nach sicherheitsrelevanten Ereignissen suchen müssen, z. B. wenn sie IT-Systeme kontrollieren oder testen, dann SOLLTEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein.

Für die Detektion von sicherheitsrelevanten Ereignissen SOLLTEN genügend personelle Ressourcen bereitgestellt werden.

DER.1.A7 Schulung von Zuständigen (S) [Vorgesetzte]

Alle Zuständigen, die Ereignismeldungen kontrollieren, SOLLTEN weiterführende Schulungen und Qualifikationen erhalten. Wenn neue IT-Komponenten beschafft werden, SOLLTE ein Budget für Schulungen eingeplant werden. Bevor die Zuständigen Schulungen für neue IT-Komponenten bekommen, SOLLTE ein Schulungskonzept erstellt werden.

DER.1.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

DER.1.A9 Einsatz zusätzlicher Detektionssysteme (S) [Fachverantwortliche]

Anhand des Netzplans SOLLTE festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen. Der Informationsverbund SOLLTE um zusätzliche Detektionssysteme und Sensoren ergänzt werden. Schadcodedetektionssysteme SOLLTEN eingesetzt und zentral verwaltet werden. Auch die im Netzplan definierten Übergange zwischen internen und externen Netzen SOLLTEN um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

DER.1.A10 Einsatz von TLS-/SSL-Proxies (S) [Fachverantwortliche]

An den Übergängen zu externen Netzen SOLLTEN TLS-/SSL-Proxies eingesetzt werden, welche die verschlüsselte Verbindung unterbrechen und es so ermöglichen, die übertragenen Daten auf Malware zu prüfen. Alle TLS-/SSL-Proxies SOLLTEN vor unbefugten Zugriffen geschützt werden. Auf den TLS-/SSL-Proxies SOLLTEN sicherheitsrelevante Ereignisse automatisch detektiert werden. Es SOLLTE eine organisatorische Regelung erstellt werden, unter welchen datenschutzrechtlichen Voraussetzungen die Logdaten manuell ausgewertet werden dürfen.

DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse (S) [Fachverantwortliche]

Die auf einer zentralen Protokollinfrastruktur gespeicherten Ereignismeldungen der IT-Systeme und Anwendungen (siehe OPS.1.1.5 *Protokollierung*) SOLLTEN mithilfe eines Tools abgerufen werden können. Mit dem auswählten Tool SOLLTEN die Meldungen ausgewertet werden können. Die gesammelten Ereignismeldungen SOLLTEN regelmäßig auf Auffälligkeiten kontrolliert werden. Die Signaturen der Detektionssysteme SOLLTEN immer aktuell und auf dem gleichen Stand sein, damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können.

DER.1.A12 Auswertung von Informationen aus externen Quellen (S) [Fachverantwortliche]

Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, SOLLTEN externe Quellen herangezogen werden. Meldungen über unterschiedliche Kanäle SOLLTEN von den Mitarbeitenden auch als relevant erkannt und an die richtige Stelle weitergeleitet werden. Informationen aus zuverlässigen Quellen SOLLTEN grundsätzlich ausgewertet werden. Alle gelieferten Informationen SOLLTEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind. Ist dies der Fall, SOLLTEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.

DER.1.A13 Regelmäßige Audits der Detektionssysteme (S)

Die vorhandenen Detektionssysteme und getroffenen Maßnahmen SOLLTEN in regelmäßigen Audits daraufhin überprüft werden, ob sie noch aktuell und wirksam sind. Es SOLLTEN die Messgrößen ausgewertet werden, die beispielsweise anfallen, wenn sicherheitsrelevante Ereignisse aufgenommen, gemeldet und eskaliert werden. Die Ergebnisse der Audits SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

DER.1.A14 Auswertung der Protokollierungsdaten durch spezialisiertes Personal (H)

Es SOLLTEN Mitarbeitende speziell damit beauftragt werden, alle Protokollierungsdaten zu überwachen. Die Überwachung der Protokollierungsdaten SOLLTE die überwiegende Aufgabe der beauftragten Mitarbeitenden sein. Die beauftragten Mitarbeitenden SOLLTEN spezialisierte weiterführende Schulungen und Qualifikationen erhalten. Ein Personenkreis SOLLTE benannt werden, der ausschließlich für das Thema Auswertung von Protokollierungsdaten verantwortlich ist.

DER.1.A15 Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen (H)

Zentrale Komponenten SOLLTEN eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale, automatisierte Analysen mit Softwaremitteln SOLLTEN eingesetzt werden. Mit diesen zentralen, automatisierten Analysen mit Softwaremitteln SOLLTEN alle in der Systemumgebung anfallenden Ereignisse aufgezeichnet und in Bezug zueinander gesetzt werden. Die sicherheitsrelevanten Vorgänge SOLLTEN sichtbar gemacht werden. Alle eingelieferten Daten SOLLTEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die Daten SOLLTEN möglichst permanent ausgewertet werden. Werden definierte Schwellwerte überschritten, SOLLTE automatisch alarmiert werden. Das Personal SOLLTE sicherstellen, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. In diesem Zusammenhang SOLLTEN auch die betroffenen Mitarbeitenden sofort informiert werden.

Die Systemverantwortlichen SOLLTEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist. Zusätzlich SOLLTEN bereits überprüfte Daten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.

DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen (H)

Anwendungen mit erhöhtem Schutzbedarf SOLLTEN durch zusätzliche Detektionsmaßnahmen geschützt werden. Dafür SOLLTEN z. B. solche Detektionssysteme eingesetzt werden, mit denen sich der erhöhte Schutzbedarf technisch auch sicherstellen lässt.

DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse (H)

Bei einem sicherheitsrelevanten Ereignis SOLLTEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und mit geeigneten Schutzmaßnahmen reagieren. Hierbei SOLLTEN Verfahren eingesetzt werden, die automatisch mögliche Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen erkennen. Es SOLLTE möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden.

DER.1.A18 Durchführung regelmäßiger Integritätskontrollen (H)

Alle Detektionssysteme SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch integer sind. Auch SOLLTEN die Berechtigungen der Benutzenden kontrolliert werden. Zusätzlich SOLLTEN die Sensoren eine Integritätskontrolle von Dateien durchführen. Bei sich ändernden Werten SOLLTE eine automatische Alarmierung ausgelöst werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) regelt in seinem Mindeststandard „Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen" die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen (SRE). Die Mindeststandards sind von den in § 8 Abs. 1 Satz 1 BSIG genannten Stellen der Bundesverwaltung umzusetzen.

Das BSI hat das weiterführende Dokument „BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, Version 1.0" zum Themenfeld Intrusion Detection veröffentlicht.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security" im Kapitel TS1.5 Intrusion Detection Vorgaben für den Einsatz von Intrusion Detection Systemen.

Bundesamt
für Sicherheit in der
Informationstechnik

DER.2.1 Behandlung von Sicherheitsvorfällen

1. Beschreibung

1.1. Einleitung

Um Schäden zu begrenzen und um weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren (Security Incident Handling oder auch Security Incident Response).

Ein Sicherheitsvorfall kann sich stark auf eine Institution auswirken und große Schäden nach sich ziehen. Solche Vorfälle sind beispielsweise Fehlkonfigurationen, die dazu führen, dass vertrauliche Informationen offengelegt werden, oder kriminelle Handlungen, wie z. B. Angriffe auf Server, der Diebstahl von vertraulichen Informationen sowie Sabotage oder Erpressung mit IT-Bezug.

Die Ursachen für Sicherheitsvorfälle sind vielfältig, so spielen unter anderem Malware, veraltete Systeminfrastrukturen sowie Innentäter und Innentäterinnen eine Rolle. Angreifende nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, für die es noch keinen Patch gibt. Eine weitere ernstzunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT).

Außerdem könnten sich Benutzende, der IT-Betrieb oder externe Dienstleistende falsch verhalten, sodass Systemparameter sicherheitskritisch geändert werden oder sie gegen interne Richtlinien verstoßen. Weiter ist als Ursache denkbar, dass Zugriffsrechte verletzt werden, dass Software und Hardware geändert oder schutzbedürftige Räume und Gebäude unzureichend gesichert werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, einen systematischen Weg aufzuzeigen, wie ein Konzept zur Behandlung von Sicherheitsvorfällen erstellt werden kann.

1.3. Abgrenzung und Modellierung

Der Baustein DER.2.1 *Behandlung von Sicherheitsvorfällen* ist für den Informationsverbund einmal anzuwenden.

Der Fokus dieses Bausteins liegt auf der Behandlung von Sicherheitsvorfällen aus Sicht der Informationstechnik. Bevor Sicherheitsvorfälle behandelt werden können, müssen sie jedoch erkannt werden. Sicherheitsanforderungen dazu sind im Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* enthalten und werden im vorliegenden Baustein vorausgesetzt. Die Vorsorgemaßnahmen, die notwendig sind, um IT-forensische Untersuchungen zu ermöglichen, sind im Baustein DER.2.2 *Vorsorge für die IT-Forensik* beschrieben. Die Bereinigung nach einem APT-Vorfall ist Thema im Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle*. Ein besonderer Bereich der Behandlung von Sicherheitsvorfällen ist das Notfallmanagement, das im Baustein DER.4 *Notfallmanagement* thematisiert und hier nicht weiter betrachtet wird. Es ist jedoch zu beachten, dass die Entscheidung darüber, ob ein Notfall vorliegt oder nicht, im vorliegenden Baustein getroffen wird.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein DER.2.1 *Behandlung von Sicherheitsvorfällen* von besonderer Bedeutung.

2.1. Ungeeigneter Umgang mit Sicherheitsvorfällen

In der Praxis kann nie ausgeschlossen werden, dass Sicherheitsvorfälle auftreten. Das gilt auch dann, wenn viele Sicherheitsmaßnahmen umgesetzt sind. Wird auf akute Sicherheitsvorfälle jedoch nicht oder nicht angemessen reagiert, können daraus große Schäden mit katastrophalen Folgen entstehen. Beispiele hierfür sind:

- In den Protokolldateien einer Firewall finden sich auffällige Einträge. Wird nicht zeitnah untersucht, ob dies erste Anzeichen für einen Einbruchsversuch sind, können Angreifende die Firewall mit einem erfolgreichen Angriff unbemerkt überwinden und in das interne Netz der Institution eindringen.
- Es werden Sicherheitslücken in den verwendeten IT-Systemen bzw. Anwendungen bekannt. Beschafft sich die Institution diese Informationen nicht rechtzeitig und leitet sie die notwendigen Gegenmaßnahmen nicht zügig ein, können diese Sicherheitslücken bei einem Angriff ausgenutzt werden.
- Ein Einbruchdiebstahl in einer Filiale wird für einen Fall von Beschaffungskriminalität gehalten, da Notebooks und Flachbildschirme entwendet wurden. Der Tatsache, dass sich auf den Notebooks vertrauliche Informationen und Zugangsdaten für IT-Systeme im Intranet befunden haben, wird keine größere Bedeutung beigemessen. Der oder die Informationssicherheitsbeauftragte (ISB) wird daher nicht informiert. Auf die nachfolgenden Angriffe auf die IT-Systeme anderer Standorte und der Firmenzentrale ist die Institution daher nicht vorbereitet. Für den Angriff wurden die auf den gestohlenen Notebooks gefundenen Daten verwendet.

Wenn für den Umgang mit Sicherheitsvorfällen keine geeignete Vorgehensweise vorgegeben ist, können in Eile und unter Stress falsche Entscheidungen getroffen werden. Diese können z. B. dazu führen, dass die Presse falsch informiert wird. Außerdem könnten Dritte durch die eigenen IT-Systeme geschädigt werden und Schadenersatz fordern. Auch ist es möglich, dass keinerlei Ausweich- oder Wiederherstellungsmaßnahmen vorgesehen sind und sich somit der Schaden für die Institution deutlich erhöht.

2.2. Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen

Wenn nach einem Sicherheitsvorfall unvorsichtig oder nicht nach Vorgaben gehandelt wird, kann das dazu führen, dass wichtige Beweisspuren für die Aufklärung oder die spätere juristische Verfolgung unbeabsichtigt zerstört oder nicht gerichtsverwertbar gemacht werden.

Beispiele hierfür sind:

- Auf einem Client wurde bei einem Angriff eine Schadsoftware platziert, deren Arbeitsweise und Ziel nur im laufenden Zustand analysiert werden kann. Dafür müssten Informationen über die aktiven Prozesse und der Inhalt des Hauptspeichers gesichert und ausgewertet werden. Wird der Client nun voreilig heruntergefahren, können die Informationen nicht mehr für eine Analyse und Aufklärung des Sicherheitsvorfalls herangezogen werden.
- Der IT-Betrieb findet auf einem Server einen laufenden Prozess, der eine überdurchschnittliche CPU-Auslastung verursacht. Zusätzlich erzeugt dieser Prozess temporäre Dateien und versendet unbekannte Informationen über das Internet. Wird der Prozess voreilig beendet und werden die temporären Dateien einfach gelöscht, kann nicht herausgefunden werden, ob vertrauliche Informationen entwendet wurden.
- Ein wichtiger Server wird kompromittiert, weil der IT-Betrieb durch die starke Arbeitsbelastung und ein fehlendes Wartungsfenster die letzten Sicherheitsupdates nicht wie geplant einspielen konnte. Um möglichen disziplinarischen Konsequenzen zu entgehen, spielt der IT-Betrieb die fehlenden Updates ein, bevor ein Sicherheitsteam die Einbruchsursache und den entstandenen Schaden analysieren kann. Eine mangelhafte Fehlerkultur hat somit eine Analyse des Problems verhindert.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.2.1 *Behandlung von Sicherheitsvorfällen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	IT-Betrieb, Institutionsleitung, Fachverantwortliche, Datenschutzbeauftragte, Notfallbeauftragte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

DER.2.1.A1 Definition eines Sicherheitsvorfalls (B)

In einer Institution MUSS klar definiert sein, was ein Sicherheitsvorfall ist. Ein Sicherheitsvorfall MUSS so weit wie möglich von Störungen im Tagesbetrieb abgegrenzt sein. Alle an der Behandlung von Sicherheitsvorfällen beteiligten Mitarbeitenden MÜSSEN die Definition eines Sicherheitsvorfalls kennen. Die Definition und die Eintrittsschwellen eines solchen Vorfalls SOLLTEN sich nach dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Systeme bzw. Anwendungen richten.

DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen (B)

Eine Richtlinie zur Behandlung von Sicherheitsvorfällen MUSS erstellt werden. Darin MÜSSEN Zweck und Ziel der Richtlinie definiert sowie alle Aspekte der Behandlung von Sicherheitsvorfällen geregelt werden. So MÜSSEN Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen beschrieben sein. Zusätzlich MUSS es für alle Mitarbeitenden zielgruppenorientierte und praktisch anwendbare Handlungsanweisungen geben. Weiterhin SOLLTEN die Schnittstellen zu anderen Managementbereichen berücksichtigt werden, z. B. zum Notfallmanagement.

Die Richtlinie MUSS allen Mitarbeitenden bekannt sein. Sie MUSS mit dem IT-Betrieb abgestimmt und durch die Institutionsleitung verabschiedet sein. Die Richtlinie MUSS regelmäßig geprüft und aktualisiert werden.

DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpersonen bei Sicherheitsvorfällen (B)

Es MUSS geregelt werden, wer bei Sicherheitsvorfällen wofür verantwortlich ist. Für alle Mitarbeitenden MÜSSEN die Aufgaben und Kompetenzen bei Sicherheitsvorfällen festgelegt werden. Insbesondere Mitarbeitende, die Sicherheitsvorfälle bearbeiten sollen, MÜSSEN über ihre Aufgaben und Kompetenzen unterrichtet werden. Dabei MUSS auch geregelt sein, wer die mögliche Entscheidung für eine forensische Untersuchung trifft, nach welchen Kriterien diese vorgenommen wird und wann sie erfolgen soll.

Die Ansprechpartner oder Ansprechpartnerinnen für alle Arten von Sicherheitsvorfällen MÜSSEN den Mitarbeitenden bekannt sein. Kontaktinformationen MÜSSEN immer aktuell und leicht zugänglich sein.

DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen (B) [Institutionsleitung, IT-Betrieb, Datenschutzbeauftragte, Notfallbeauftragte]

Von einem Sicherheitsvorfall MÜSSEN alle betroffenen internen und externen Stellen zeitnah informiert werden. Dabei MUSS geprüft werden, ob der oder die Datenschutzbeauftragte, der Betriebs- und Personalrat sowie Mitarbeitende aus der Rechtsabteilung einbezogen werden müssen. Ebenso MÜSSEN die Meldepflichten für Behörden und regulierte Branchen berücksichtigt werden. Außerdem MUSS gewährleistet sein, dass betroffene Stellen über die erforderlichen Maßnahmen informiert werden.

DER.2.1.A5 Behebung von Sicherheitsvorfällen (B) [IT-Betrieb]

Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, MÜSSEN die Zuständigen zunächst das Problem eingrenzen und die Ursache finden. Danach MÜSSEN die erforderlichen Maßnahmen auswählt werden, um das Problem zu beheben. Die Leitung des IT-Betriebs MUSS eine Freigabe erteilen, bevor die Maßnahmen umgesetzt werden. Anschließend MUSS die Ursache beseitigt und ein sicherer Zustand hergestellt werden.

Eine aktuelle Liste von internen und externen Sicherheitsfachleuten MUSS vorhanden sein, die bei Sicherheitsvorfällen für Fragen aus den erforderlichen Themenbereichen hinzugezogen werden können. Es MÜSSEN sichere Kommunikationsverfahren mit diesen internen und externen Stellen etabliert werden.

DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen (B) [IT-Betrieb]

Nach einem Sicherheitsvorfall MÜSSEN die betroffenen Komponenten vom Netz genommen werden. Zudem MÜSSEN alle erforderlichen Daten gesichert werden, die Aufschluss über die Art und Ursache des Problems geben könnten. Auf allen betroffenen Komponenten MÜSSEN das Betriebssystem und alle Applikationen auf Veränderungen untersucht werden.

Die Originaldaten MÜSSEN von schreibgeschützten Datenträgern wieder eingespielt werden. Dabei MÜSSEN alle sicherheitsrelevanten Konfigurationen und Patches mit aufgespielt werden. Wenn Daten aus Datensicherungen wieder eingespielt werden, MUSS sichergestellt sein, dass diese vom Sicherheitsvorfall nicht betroffen waren. Nach einem Angriff MÜSSEN alle Zugangsdaten auf den betroffenen Komponenten geändert werden, bevor sie wieder in Betrieb genommen werden. Die betroffenen Komponenten SOLLTEN einem Penetrationstest unterzogen werden, bevor sie wieder eingesetzt werden.

Bei der Wiederherstellung der sicheren Betriebsumgebung MÜSSEN die Benutzenden in die Anwendungsfunktionstests einbezogen werden. Nachdem alles wiederhergestellt wurde, MÜSSEN die Komponenten inklusive der Netzübergänge gezielt überwacht werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen (S) [Institutionsleitung]

Es SOLLTE eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen definiert werden. Die Abläufe, Prozesse und Vorgaben für die verschiedenen Sicherheitsvorfälle SOLLTEN dabei eindeutig geregelt und geeignet dokumentiert werden. Die Institutionsleitung SOLLTE die festgelegte Vorgehensweise in Kraft setzen und allen Beteiligten zugänglich machen. Es SOLLTE regelmäßig überprüft werden, ob die Vorgehensweise noch aktuell und wirksam ist. Bei Bedarf SOLLTE die Vorgehensweise angepasst werden.

DER.2.1.A8 Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen (S)

Für den Umgang mit Sicherheitsvorfällen SOLLTEN geeignete Organisationsstrukturen festgelegt werden. Es SOLLTE ein Sicherheitsvorfall-Team aufgebaut werden, dessen Mitglieder je nach Art des Vorfalls einberufen werden können. Auch wenn das Sicherheitsvorfall-Team nur für einen konkreten Fall zusammentritt, SOLLTEN bereits im Vorfeld geeignete Mitglieder benannt und in ihre Aufgaben eingewiesen sein. Es SOLLTE regelmäßig geprüft werden, ob die Zusammensetzung des Sicherheitsvorfall-Teams noch angemessen ist. Gegebenenfalls SOLLTE das Sicherheitsvorfall-Team neu zusammengestellt werden.

DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle (S)

Für die verschiedenen Arten von Sicherheitsvorfällen SOLLTEN die jeweils passenden Meldewege aufgebaut sein. Es SOLLTE dabei sichergestellt sein, dass Mitarbeitende Sicherheitsvorfälle über verlässliche und vertrauenswürdige Kanäle schnell und einfach melden können.

Wird eine zentrale Anlaufstelle für die Meldung von Störungen oder Sicherheitsvorfällen eingerichtet, SOLLTE dies an alle Mitarbeitende kommuniziert werden.

Eine Kommunikations- und Kontaktstrategie SOLLTE vorliegen. Darin SOLLTE geregelt sein, wer grundsätzlich informiert werden muss und wer informiert werden darf, durch wen dies in welcher Reihenfolge erfolgt und in welcher Tiefe informiert wird. Es SOLLTE definiert sein, wer Informationen über Sicherheitsvorfälle an Dritte weitergibt. Ebenso SOLLTE sichergestellt sein, dass keine unautorisierten Personen Informationen über den Sicherheitsvorfall weitergeben.

DER.2.1.A10 Eindämmen der Auswirkung von Sicherheitsvorfällen (S) [Notfallbeauftragte, IT-Betrieb]

Parallel zur Ursachenanalyse eines Sicherheitsvorfalls SOLLTE entschieden werden, ob es wichtiger ist, den entstandenen Schaden einzudämmen oder den Vorfall aufzuklären. Um die Auswirkung eines Sicherheitsvorfalls abschätzen zu können, SOLLTEN ausreichend Informationen vorliegen. Für ausgewählte Sicherheitsvorfallszenarien SOLLTEN bereits im Vorfeld Worst-Case-Betrachtungen durchgeführt werden.

DER.2.1.A11 Einstufung von Sicherheitsvorfällen (S) [IT-Betrieb]

Ein einheitliches Verfahren SOLLTE festgelegt werden, um Sicherheitsvorfälle und Störungen einzustufen. Das Einstufungsverfahren für Sicherheitsvorfälle SOLLTE zwischen Sicherheitsmanagement und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt sein.

DER.2.1.A12 Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung (S) [Notfallbeauftragte]

Die Schnittstellen zwischen Störungs- und Fehlerbehebung, Notfallmanagement und Sicherheitsmanagement SOLLTEN analysiert werden. Dabei SOLLTEN auch eventuell gemeinsam benutzbare Ressourcen identifiziert werden.

Die bei der Störungs- und Fehlerbehebung beteiligten Mitarbeitenden SOLLTEN für die Behandlung von Sicherheitsvorfällen sowie für das Notfallmanagement sensibilisiert werden. Das Sicherheitsmanagement SOLLTE lesenden Zugriff auf eingesetzte Incident-Management-Werkzeuge haben.

DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmanagement (S) [Notfallbeauftragte]

Die Behandlung von Sicherheitsvorfällen SOLLTE mit dem Notfallmanagement abgestimmt sein. Falls es in der Institution eine spezielle Rolle für Störungs- und Fehlerbehebung gibt, SOLLTE auch diese mit einbezogen werden.

DER.2.1.A14 Eskalationsstrategie für Sicherheitsvorfälle (S) [IT-Betrieb]

Über die Kommunikations- und Kontaktstrategie hinaus SOLLTE eine Eskalationsstrategie formuliert werden. Diese SOLLTE zwischen den Verantwortlichen für Störungs- und Fehlerbehebung und dem Informationssicherheitsmanagement abgestimmt werden.

Die Eskalationsstrategie SOLLTE eindeutige Handlungsanweisungen enthalten, wer auf welchem Weg bei welcher Art von erkennbaren oder vermuteten Sicherheitsstörungen wann einzubeziehen ist. Es SOLLTE geregelt sein, zu welchen Maßnahmen eine Eskalation führt und wie reagiert werden soll.

Für die festgelegte Eskalationsstrategie SOLLTEN geeignete Werkzeuge wie z. B. Ticket-Systeme ausgewählt werden. Diese SOLLTEN sich auch dafür eignen, vertrauliche Informationen zu verarbeiten. Es SOLLTE sichergestellt sein, dass die Werkzeuge auch während eines Sicherheitsvorfalls bzw. Notfalls verfügbar sind.

Die Eskalationsstrategie SOLLTE regelmäßig überprüft und gegebenenfalls aktualisiert werden. Die Checklisten (Matching Szenarios) für Störungs- und Fehlerbehebung SOLLTEN regelmäßig um sicherheitsrelevante Themen ergänzt bzw. aktualisiert werden. Die festgelegten Eskalationswege SOLLTEN in Übungen erprobt werden.

DER.2.1.A15 Schulung der Mitarbeitenden des Service Desks (S) [IT-Betrieb]

Dem Personal des Service Desks SOLLTEN geeignete Hilfsmittel zur Verfügung stehen, damit sie Sicherheitsvorfälle erkennen können. Sie SOLLTEN ausreichend geschult sein, um die Hilfsmittel selbst anwenden zu können. Die Mitarbeitenden des Service Desks SOLLTEN den Schutzbedarf der betroffenen IT-Systeme kennen.

DER.2.1.A16 Dokumentation der Behebung von Sicherheitsvorfällen (S)

Die Behebung von Sicherheitsvorfällen SOLLTE nach einem standardisierten Verfahren dokumentiert werden. Es SOLLTEN alle durchgeführten Aktionen inklusive der Zeitpunkte sowie die Protokolldaten der betroffenen Komponenten dokumentiert werden. Dabei SOLLTE die Vertraulichkeit bei der Dokumentation und Archivierung der Berichte gewährleistet sein.

Die benötigten Informationen SOLLTEN in die jeweiligen Dokumentationssysteme eingepflegt werden, bevor die Störung als beendet und als abgeschlossen markiert wird. Im Vorfeld SOLLTEN mit dem oder der ISB die dafür erforderlichen Anforderungen an die Qualitätssicherung definiert werden.

DER.2.1.A17 Nachbereitung von Sicherheitsvorfällen (S)

Sicherheitsvorfälle SOLLTEN standardisiert nachbereitet werden. Dabei SOLLTE untersucht werden, wie schnell die Sicherheitsvorfälle erkannt und behoben wurden. Weiterhin SOLLTE untersucht werden, ob die Meldewege funktionierten, ausreichend Informationen für die Bewertung verfügbar und ob die Detektionsmaßnahmen wirksam waren. Ebenso SOLLTE geprüft werden, ob die ergriffenen Maßnahmen und Aktivitäten wirksam und effizient waren.

Die Erfahrungen aus vergangenen Sicherheitsvorfällen SOLLTEN genutzt werden, um daraus Handlungsanweisungen für vergleichbare Sicherheitsvorfälle zu erstellen. Diese Handlungsanweisungen SOLLTEN den relevanten Personengruppen bekanntgegeben und auf Basis neuer Erkenntnisse regelmäßig aktualisiert werden.

Die Institutionsleitung SOLLTE jährlich über die Sicherheitsvorfälle unterrichtet werden. Besteht sofortiger Handlungsbedarf, MUSS die Institutionsleitung umgehend informiert werden.

DER.2.1.A18 Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen (S) [Fachverantwortliche]

Nachdem ein Sicherheitsvorfall analysiert wurde, SOLLTE untersucht werden, ob die Prozesse und Abläufe im Rahmen der Behandlung von Sicherheitsvorfällen geändert oder weiterentwickelt werden müssen. Dabei SOLLTEN alle Personen, die an dem Vorfall beteiligt waren, über ihre jeweiligen Erfahrungen berichten.

Es SOLLTE geprüft werden, ob es neue Entwicklungen im Bereich Incident Management und in der Forensik gibt und ob diese in die jeweiligen Dokumente und Abläufe eingebracht werden können.

Werden Hilfsmittel und Checklisten eingesetzt, z. B. für Service-Desk-Mitarbeitende, SOLLTE geprüft werden, ob diese um relevante Fragen und Informationen zu erweitern sind.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

DER.2.1.A19 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen (H) [Institutionsleitung]

Es SOLLTEN Prioritäten für die Behandlung von Sicherheitsvorfällen vorab festgelegt und regelmäßig aktualisiert werden. Dabei SOLLTE auch die vorgenommene Einstufung von Sicherheitsvorfällen berücksichtigt werden.

Die Prioritäten SOLLTEN von der Institutionsleitung genehmigt und in Kraft gesetzt werden. Sie SOLLTEN allen Verantwortlichen bekannt sein, die mit der Behandlung von Sicherheitsvorfällen zu tun haben. Die festgelegten Prioritätsklassen SOLLTEN außerdem im Incident Management hinterlegt sein.

DER.2.1.A20 Einrichtung einer dedizierten Meldestelle für Sicherheitsvorfälle (H)

Eine dedizierte Stelle zur Meldung von Sicherheitsvorfällen SOLLTE eingerichtet werden. Es SOLLTE gewährleistet sein, dass die Meldestelle zu den üblichen Arbeitszeiten erreichbar ist. Zusätzlich SOLLTE es möglich sein, dass Sicherheitsvorfälle auch außerhalb der üblichen Arbeitszeiten gemeldet werden können. Die Mitarbeitenden der Meldestelle SOLLTEN ausreichend geschult und für die Belange der Informationssicherheit sensibilisiert sein. Alle Informationen über Sicherheitsvorfälle SOLLTEN bei der Meldestelle vertraulich behandelt werden.

DER.2.1.A21 Einrichtung eines Teams von Fachleuten für die Behandlung von Sicherheitsvorfällen (H)

Es SOLLTE ein Team mit erfahrenen und vertrauenswürdigen Fachleuten zusammengestellt werden. Neben dem technischen Verständnis SOLLTEN die Teammitglieder auch über Kompetenzen im Bereich Kommunikation verfügen. Die Vertrauenswürdigkeit der Mitglieder des Teams SOLLTE überprüft werden. Die Zusammensetzung des Teams SOLLTE regelmäßig überprüft und, wenn nötig, geändert werden.

Die Mitglieder des Teams SOLLTEN in die Eskalations- und Meldewege eingebunden sein. Das Experten- und Expertinnenteam SOLLTE für die Analyse von Sicherheitsvorfällen an den in der Institution eingesetzten Systemen ausgebildet werden. Die Mitglieder des Experten- und Expertinnenteams SOLLTEN sich regelmäßig weiterbilden, sowohl zu den eingesetzten Systemen als auch zur Detektion und Reaktion auf Sicherheitsvorfälle. Dem Experten- und Expertinnenteam SOLLTEN alle vorhandenen Dokumentationen sowie finanzielle und technische Ressourcen zur Verfügung stehen, um Sicherheitsvorfälle schnell und diskret zu behandeln.

Das Experten- und Expertinnenteams SOLLTE in geeigneter Weise in den Organisationsstrukturen berücksichtigt und in diese integriert werden. Die Zuständigkeiten des Teams SOLLTEN vorher mit denen des Sicherheitsvorfall-Teams abgestimmt werden.

DER.2.1.A22 Überprüfung der Effizienz des Managementsystems zur Behandlung von Sicherheitsvorfällen (H)

Das Managementsystem zur Behandlung von Sicherheitsvorfällen SOLLTE regelmäßig daraufhin geprüft werden, ob es noch aktuell und wirksam ist. Dazu SOLLTEN sowohl angekündigte als auch unangekündigte Übungen durchgeführt werden. Die Übungen SOLLTEN vorher mit der Institutionsleitung abgestimmt sein. Es SOLLTEN die Messgrößen ausgewertet werden, die anfallen, wenn Sicherheitsvorfälle aufgenommen, gemeldet und eskaliert werden, z. B. die Zeiträume von der Erstmeldung bis zur verbindlichen Bestätigung eines Sicherheitsvorfalls.

Außerdem SOLLTEN Planspiele zur Behandlung von Sicherheitsvorfällen durchgeführt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology – Security techniques – Information security management systems – Requirements" im Anhang A16 „Information security incident management" Vorgaben für die Behandlung von Sicherheitsvorfällen.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27035:2016 „Information technology – Security techniques – Information security incident management" Vorgaben für die Behandlung von Sicherheitsvorfällen.

Das National Institute of Standards and Technology (NIST) macht in seiner Special Publication 800-61 Revision 2 „Computer Security Incident Handling Guide" generelle Vorgaben zur Behandlung von Sicherheitsvorfällen.

Das National Institute of Standards and Technology (NIST) macht in seiner Special Publication 800-83 Revision 1 „Guide to Malware incident Prevention and Handling for Desktops and Laptops" spezifische Vorgaben zum Umgang mit Malware-Infektionen bei Laptops und Desktops.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security" im Kapitel TS1.4 „Technical Security Management; Identity and Access Management" Vorgaben für die Behandlung von Sicherheitsvorfällen.

Bundesamt
für Sicherheit in der
Informationstechnik

DER.2.2 Vorsorge für die IT-Forensik

1. Beschreibung

1.1. Einleitung

IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Datennetzen zur Aufklärung von Sicherheitsvorfällen in IT-Systemen.

IT-Sicherheitsvorfälle forensisch zu untersuchen, ist immer dann notwendig, wenn entstandene Schäden bestimmt, Angriffe abgewehrt, zukünftige Angriffe vermieden und Angreifende identifiziert werden sollen. Ob ein IT-Sicherheitsvorfall forensisch untersucht wird, entscheidet sich, während der Vorfall behandelt wird. Eine IT-forensische Untersuchung im Sinne dieses Bausteins besteht aus den folgenden Phasen:

- Strategische Vorbereitung: In dieser Phase werden Prozesse geplant und aufgebaut, die sicherstellen, dass eine Institution IT-Sicherheitsvorfälle forensisch analysieren kann. Sie ist auch dann notwendig, wenn die Institution über keine eigene Forensik-Expertise verfügt.
- Initialisierung: Nachdem die verantwortlichen Mitarbeitenden entschieden haben, einen IT-Sicherheitsvorfall forensisch zu untersuchen, werden die vorher geplanten Prozesse angestoßen. Des Weiteren wird der Untersuchungsrahmen festgelegt und es werden Erstmaßnahmen durchgeführt.
- Spurensicherung: Hier werden die zu sichernden Beweismittel ausgewählt und die Daten forensisch gesichert. Dabei wird zwischen Live-Forensik und Post-Mortem-Forensik unterschieden: Die Live-Forensik stellt sicher, dass flüchtige Daten, wie z. B. Netzverbindungen oder RAM, von einem laufenden IT-System gesichert werden. Bei der Post-Mortem-Forensik hingegen werden forensische Kopien von Datenträgern erstellt.
- Analyse: Die gesammelten Daten werden forensisch analysiert. Dabei werden die Daten sowohl für sich als auch im Gesamtzusammenhang betrachtet.
- Ergebnisdarstellung: Die relevanten Untersuchungsergebnisse werden zielgruppengerecht aufbereitet und vermittelt.

1.2. Zielsetzung

Der Baustein zeigt auf, welche Vorsorgemaßnahmen notwendig sind, um IT-forensische Untersuchungen zu ermöglichen. Dabei wird vor allem darauf eingegangen, wie die Spurensicherung vorbereitet und durchgeführt werden kann.

Führen Forensik-Dienstleistende Spurensicherungen ganz oder teilweise durch, gelten die Anforderungen auch für die Dienstleistenden. Durch vertragliche Vereinbarungen und Prüfungen kann dabei sichergestellt werden, dass sich die Dienstleistenden auch daran halten.

1.3. Abgrenzung und Modellierung

Der Baustein DER.2.2 *Vorsorge für die IT-Forensik* ist für den gesamten Informationsverbund einmal anzuwenden.

Der Baustein befasst sich mit Vorsorgemaßnahmen, die grundlegend für spätere IT-forensische Untersuchungen sind.

Wie die eigentliche forensische Analyse durchgeführt wird, ist daher nicht Thema dieses Bausteins. Es werden keine Anforderungen beschrieben, die sicherstellen, dass Angriffe erkannt werden. Diese sind im Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* enthalten und werden im vorliegenden Baustein vorausgesetzt. Auch werden keine Kriterien und Prozesse erläutert, anhand derer die Verantwortlichen entscheiden können, ob ein IT-

Sicherheitsvorfall forensisch untersucht werden muss oder nicht. Die Entscheidung darüber wird getroffen, während der Sicherheitsvorfall behandelt wird (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Ebenso bezieht sich der Baustein nicht auf IT-forensische Untersuchungen bei Straftaten.

Letztlich geht der Baustein auch nicht darauf ein, wie sich IT-Infrastrukturen bereinigen lassen, nachdem sie angegriffen worden sind (siehe dazu DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle*). Die dort beschriebenen Tätigkeiten können jedoch durch die Ergebnisse von IT-forensischen Untersuchungen maßgeblich unterstützt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein DER.2.2 *Vorsorge für die IT-Forensik* von besonderer Bedeutung.

2.1. Verstoß gegen rechtliche Rahmenbedingungen

Für IT-forensische Untersuchungen werden oft alle für notwendig befundenen Daten kopiert, sichergestellt und ausgewertet. Darunter befinden sich meistens auch personenbezogene Daten von Mitarbeitenden oder externen Partner und Partnerinnen. Wird darauf z. B. unbegründet und ohne Einbeziehung der oder die Datenschutzbeauftragte zugegriffen, verstößt die Institution gegen gesetzliche Regelungen, etwa wenn dabei die Zweckbindung missachtet wird. Auch ist es möglich, dass aus den erhobenen Daten beispielsweise abgeleitet werden kann, wie sich Mitarbeitende verhalten, oder es kann ein Bezug zu ihnen hergestellt werden. Dadurch besteht die Gefahr, dass auch gegen interne Regelungen verstoßen wird.

2.2. Verlust von Beweismitteln durch fehlerhafte oder unvollständige Beweissicherung

Werden Beweismittel falsch oder nicht schnell genug gesichert, können dadurch wichtige Daten verloren gehen, die später nicht wiederhergestellt werden können. Im ungünstigsten Fall führt das zu einer ergebnislosen forensischen Untersuchung. Mindestens ist jedoch die Beweiskraft eingeschränkt.

Die Gefahr, wichtige Beweismittel zu verlieren, steigt stark an, wenn Mitarbeitende die Werkzeuge zur Forensik fehlerhaft benutzen, Daten zu langsam sichern oder zu wenig üben. Oft gehen auch Beweismittel verloren, wenn die Verantwortlichen flüchtige Daten nicht als relevant erkennen und sichern.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.2.2 *Vorsorge für die IT-Forensik* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Fachverantwortliche, Datenschutzbeauftragte, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden:

DER.2.2.A1 Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit (B) [Datenschutzbeauftragte, Institutionsleitung]

Werden Daten für forensische Untersuchungen erfasst und ausgewertet, MÜSSEN alle rechtlichen und regulatorischen Rahmenbedingungen identifiziert und eingehalten werden (siehe ORP.5 *Compliance Management (Anforderungsmanagement)*). Auch DARF NICHT gegen interne Regelungen und Mitarbeitendenvereinbarungen verstoßen werden. Dazu MÜSSEN der Betriebs- oder Personalrat sowie der oder die Datenschutzbeauftragte einbezogen werden.

DER.2.2.A2 Erstellung eines Leitfadens für Erstmaßnahmen bei einem IT-Sicherheitsvorfall (B)

Es MUSS ein Leitfaden erstellt werden, der für die eingesetzten IT-Systeme beschreibt, welche Erstmaßnahmen bei einem IT-Sicherheitsvorfall durchgeführt werden müssen, um möglichst wenig Spuren zu zerstören. Darin MUSS auch beschrieben sein, durch welche Handlungen potenzielle Spuren vernichtet werden könnten und wie sich das vermeiden lässt.

DER.2.2.A3 Vorauswahl von Forensik-Dienstleistenden (B)

Verfügt eine Institution nicht über ein eigenes Forensik-Team, MÜSSEN bereits in der Vorbereitungsphase mögliche geeignete Forensik-Dienstleistende identifiziert werden. Welche Forensik-Dienstleistenden infrage kommen, MUSS dokumentiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.2.2.A4 Festlegung von Schnittstellen zum Krisen- und Notfallmanagement (S)

Die Schnittstellen zwischen IT-forensischen Untersuchungen und dem Krisen- und Notfallmanagement SOLLTEN definiert und dokumentiert werden. Hierzu SOLLTE geregelt werden, welche Mitarbeitenden für welche Aufgaben verantwortlich sind und wie mit ihnen kommuniziert werden soll. Darüber hinaus SOLLTE sichergestellt werden, dass die zuständigen Kontaktpersonen stets erreichbar sind.

DER.2.2.A5 Erstellung eines Leitfadens für Beweissicherungsmaßnahmen bei IT-Sicherheitsvorfällen (S)

Es SOLLTE ein Leitfaden erstellt werden, in dem beschrieben wird, wie Beweise gesichert werden sollen. Darin SOLLTEN Vorgehensweisen, technische Werkzeuge, rechtliche Rahmenbedingungen und Dokumentationsvorgaben aufgeführt werden.

DER.2.2.A6 Schulung des Personals für die Umsetzung der forensischen Sicherung (S)

Alle verantwortlichen Mitarbeitenden SOLLTEN wissen, wie sie Spuren korrekt sichern und die Werkzeuge zur Forensik richtig einsetzen. Dafür SOLLTEN geeignete Schulungen durchgeführt werden.

DER.2.2.A7 Auswahl von Werkzeugen zur Forensik (S)

Es SOLLTE sichergestellt werden, dass Werkzeuge, mit denen Spuren forensisch gesichert und analysiert werden, auch dafür geeignet sind. Bevor ein Werkzeug zur Forensik eingesetzt wird, SOLLTE zudem geprüft werden, ob es richtig funktioniert. Auch SOLLTE überprüft und dokumentiert werden, dass es nicht manipuliert wurde.

DER.2.2.A8 Auswahl und Reihenfolge der zu sichernden Beweismittel (S) [Fachverantwortliche]

Eine forensische Untersuchung SOLLTE immer damit beginnen, die Ziele bzw. den Arbeitsauftrag zu definieren. Die Ziele SOLLTEN möglichst konkret formuliert sein. Danach SOLLTEN alle notwendigen Datenquellen identifiziert werden. Auch SOLLTE festgelegt werden, in welcher Reihenfolge die Daten gesichert werden und wie genau dabei vorgegangen werden soll. Die Reihenfolge SOLLTE sich danach richten, wie flüchtig (volatil) die zu sichernden Daten sind. So SOLLTEN schnell flüchtige Daten zeitnah gesichert werden. Erst danach SOLLTEN nichtflüchtige Daten wie beispielsweise Festspeicherinhalte und schließlich Backups folgen.

DER.2.2.A9 Vorauswahl forensisch relevanter Daten (S) [Fachverantwortliche]

Es SOLLTE festgelegt werden, welche sekundären Daten (z. B. Logdaten oder Verkehrsmitschnitte) auf welche Weise und wie lange im Rahmen der rechtlichen Rahmenbedingungen für mögliche forensische Beweissicherungsmaßnahmen vorgehalten werden.

DER.2.2.A10 IT-forensische Sicherung von Beweismitteln (S) [Fachverantwortliche]

Datenträger SOLLTEN möglichst komplett forensisch dupliziert werden. Wenn das nicht möglich ist, z. B. bei flüchtigen Daten im RAM oder in SAN-Partitionen, SOLLTE eine Methode gewählt werden, die möglichst wenige Daten verändert.

Die Originaldatenträger SOLLTEN versiegelt aufbewahrt werden. Es SOLLTEN schriftlich dokumentierte kryptografische Prüfsummen von den Datenträgern angelegt werden. Diese SOLLTEN getrennt und in mehreren Kopien aufbewahrt werden. Zudem SOLLTE sichergestellt sein, dass die so dokumentierten Prüfsummen nicht verändert werden können. Damit die Daten gerichtlich verwertbar sind, SOLLTE ein Zeuge bestätigen, wie dabei vorgegangen wurde und die erstellten Prüfsummen beglaubigen.

Es SOLLTE ausschließlich geschultes Personal (siehe DER.2.2.A6 *Schulung des Personals für die Umsetzung der forensischen Sicherung*) oder ein Forensik-Dienstleistender (siehe DER.2.2.A3 *Vorauswahl von Forensik-Dienstleistenden*) eingesetzt werden, um Beweise forensisch zu sichern.

DER.2.2.A11 Dokumentation der Beweissicherung (S) [Fachverantwortliche]

Wenn Beweise forensisch gesichert werden, SOLLTEN alle durchgeführten Schritte dokumentiert werden. Die Dokumentation SOLLTE lückenlos nachweisen, wie mit den gesicherten Originalbeweismitteln umgegangen wurde. Auch SOLLTE dokumentiert werden, welche Methoden eingesetzt wurden und warum sich die Verantwortlichen dafür entschieden haben.

DER.2.2.A12 Sichere Verwahrung von Originaldatenträgern und Beweismitteln (S) [Fachverantwortliche]

Alle sichergestellten Originaldatenträger SOLLTEN physisch so gelagert werden, dass nur ermittelnde und namentlich bekannte Mitarbeitende darauf zugreifen können. Wenn Originaldatenträger und Beweismittel eingelagert werden, SOLLTE festgelegt werden, wie lange sie aufzubewahren sind. Nachdem die Frist abgelaufen ist, SOLLTE geprüft werden, ob die Datenträger und Beweise noch weiter aufbewahrt werden müssen. Nach der Aufbewahrungsfrist SOLLTEN Beweismittel sicher gelöscht oder vernichtet und Originaldatenträger zurückgegeben werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

DER.2.2.A13 Rahmenverträge mit externen Dienstleistenden (H)

Die Institution SOLLTE Abrufvereinbarungen bzw. Rahmenverträge mit Forensik-Dienstleistenden abschließen, damit IT-Sicherheitsvorfälle schneller forensisch untersucht werden können.

DER.2.2.A14 Festlegung von Standardverfahren für die Beweissicherung (H)

Für Anwendungen, IT-Systeme bzw. IT-Systemgruppen mit hohem Schutzbedarf sowie für verbreitete Systemkonfigurationen SOLLTEN Standardverfahren erstellt werden, die es erlauben, flüchtige und nichtflüchtige Daten möglichst vollständig forensisch zu sichern.

Die jeweiligen systemspezifischen Standardverfahren SOLLTEN durch erprobte und möglichst automatisierte Prozesse umgesetzt werden. Sie SOLLTEN zudem durch Checklisten und technische Hilfsmittel unterstützt werden, z. B. durch Software, Software-Tools auf mobilen Datenträgern und IT-forensische Hardware wie Schreibblocker.

DER.2.2.A15 Durchführung von Übungen zur Beweissicherung (H)

Alle an forensischen Analysen beteiligten Mitarbeitenden SOLLTEN regelmäßig in Form von Übungen trainieren, wie Beweise bei einem IT-Sicherheitsvorfall zu sichern sind.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI gibt in dem „Leitfaden IT-Forensik" weiterführende Informationen in die Thematik und kann auch als Nachschlagewerk für einzelne praxisbezogene Problemstellungen dienen.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27042:2015 und 27043:2015 01:2013 Vorgaben für die Durchführung von forensischen Analysen.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security" im Kapitel TM 2.4 Forensik Investigations Vorgaben für die Durchführung von forensischen Analysen.

Der Request for Comments (RFC) 3227 „Guidelines for Evidence Collection and Archiving" gibt in seinem Leitfaden Hinweise zur grundlegenden Vorgehensweise bei einer forensischen Sicherung.

Bundesamt
für Sicherheit in der
Informationstechnik

DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

1. Beschreibung

1.1. Einleitung

Bei Advanced Persistent Threats (APTs) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen. Dabei verschaffen sich Angreifende dauerhaften Zugriff zu einem Netz und weiten diesen Zugriff auf weitere IT-Systeme aus. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und umfassende technische Fähigkeiten auf Seiten der Angreifenden aus. Angriffe dieser Art sind in der Regel schwierig zu detektieren.

Nachdem ein APT-Angriff entdeckt wurde, stehen die Zuständigen in den betroffenen Institutionen vor großen Herausforderungen. Denn sie müssen eine Bereinigung durchführen, die über das übliche Vorgehen zur Behandlung von IT-Sicherheitsvorfällen hinausgeht. Es ist davon auszugehen, dass die entdeckten Angreifenden bereits seit längerer Zeit auf die betroffene IT-Infrastruktur zugreifen können. Außerdem nutzen sie komplexe Angriffswerkzeuge, um die Standard-Sicherheitsmechanismen zu umgehen und diverse Hintertüren zu etablieren. Zudem besteht die Gefahr, dass die Angreifenden die infizierte Umgebung genau beobachten und auf Versuche zur Bereinigung reagieren, indem sie ihre Spuren verwischen und die Untersuchung sabotieren.

In diesem Baustein wird von einer hohen Bedrohungslage durch einen gezielten Angriff hochmotivierter Personen mit überdurchschnittlichen Ressourcen ausgegangen. In der Praxis ist es üblich, dass bei einem solchen Vorfall immer auch auf (zertifizierte) forensische Dienstleistung zurückgegriffen wird, wenn die Institution selbst nicht über entsprechende eigene forensische Expertise verfügt. Forensikdienstleistende werden dabei bereits in der Phase der forensischen Analyse herangezogen. Die Dienstleistenden werden jedoch auch bei der Bereinigung zumindest beratend einbezogen.

1.2. Zielsetzung

Dieser Baustein beschreibt, wie eine Institution vorgehen sollte, um nach einem APT-Angriff die IT-Systeme zu bereinigen und den regulären und sicheren Betriebszustand des Informationsverbunds wiederherzustellen.

1.3. Abgrenzung und Modellierung

Der Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* ist immer dann anzuwenden, wenn nach einem APT-Vorfall die IT-Systeme bereinigt werden sollen, um den regulären und sicheren Betriebszustand eines Informationsverbunds wiederherzustellen. Der Baustein ist auf den Informationsverbund anzuwenden.

Ein Informationsverbund kann nur bereinigt werden, wenn der APT-Vorfall vorher erfolgreich detektiert und forensisch analysiert wurde. Detektion und Forensik sind jedoch nicht Thema dieses Bausteins. Diese Themen werden in den Bausteinen DER.1 *Detektion von sicherheitsrelevanten Ereignissen* bzw. DER.2.2 *Vorsorge für die IT-Forensik* behandelt.

Im vorliegenden Baustein geht es ausschließlich um die Bereinigung von APT-Vorfällen. Andere Vorfälle werden im Baustein DER.2.1 *Behandlung von Sicherheitsvorfällen* behandelt. Auch beschreibt der Baustein nicht, wie sogenannte Indicators of Compromise (IOCs), also Einbruchsspuren, abzuleiten sind und wie diese benutzt werden können, um wiederkehrende Angreifende zu erkennen. Ebenso wird nicht darauf eingegangen, wie sich eventuell bei der Analyse und Bereinigung übersehene Hintertüren finden lassen.

Es werden ausschließlich Cyber-Angriffe berücksichtigt. Das heißt, es werden keine Angriffe betrachtet, mit denen sich z. B. physischen Zugriff auf den Informationsverbund verschafft wird. So werden Angriffsformen, bei denen in Rechenzentren eingebrochen, Administrierende bestochen, neu beschaffte Hardware abgefangen und manipuliert oder elektromagnetische Strahlung abgehört werden, nicht in diesem Baustein betrachtet.

Bereinigen Forensikdienstleistende die IT-Systeme ganz oder teilweise, gelten die Anforderungen dieses Bausteins auch für diese Dienstleistenden. Durch vertragliche Vereinbarungen und Prüfungen kann dabei sichergestellt werden, dass sich die Dienstleistenden auch daran halten (siehe OPS.2.3 *Nutzung von Outsourcing*).

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* von besonderer Bedeutung.

2.1. Unvollständige Bereinigung

APT-Angreifende wollen üblicherweise einen Informationsverbund dauerhaft infiltrieren. Sie verfügen über die dafür notwendigen Ressourcen und sind in der Lage, langfristige Angriffskampagnen durchzuführen. Dafür benutzen sie Werkzeuge und Methoden, die auf ihr Angriffsziel abgestimmt sind. Auch wenn ein APT-Vorfall entdeckt wird, kann nicht davon ausgegangen werden, dass sämtliche Zugangswege der Angreifenden gefunden, alle Infektionen und Kommunikationswege von Schadsoftware beseitigt und alle Hintertüren entfernt wurden. Bei einer unvollständigen Bereinigung ist es jedoch sehr wahrscheinlich, dass Angreifende zu einem späteren Zeitpunkt, z. B. nach einer längeren Ruhephase, erneut auf die IT-Systeme zugreifen und ihren Zugang wieder ausbauen. Das können sie beispielsweise, indem sie Hintertüren nicht nur in Betriebssystemen und Anwendungssoftware platzieren, sondern auch hardwarenahe Komponenten wie etwa Firmware manipulieren. Solche Modifikationen sind sehr schwer zu identifizieren und das notwendige Wissen, um sie zu extrahieren und zu analysieren, ist nur wenig verbreitet. Versuchen die Zuständigen z. B. die IT-Komponenten zu bereinigen, indem sie die Firmware überschreiben oder aktualisieren, kann es trotzdem passieren, dass die Angreifenden auch die Update-Routinen modifiziert haben. Auf diesem Weg können sie dann wieder auf die IT-Systeme zugreifen.

2.2. Vernichtung von Spuren

Nach einem APT-Vorfall werden IT-Systeme oft neu installiert oder ganz ausgemustert. Wurde jedoch zuvor von den IT-Systemen keine forensische Kopie angefertigt, können Spuren vernichtet werden, die für eine weitere Aufklärung des Vorfalls oder sogar für ein Gerichtsverfahren notwendig wären.

2.3. Vorzeitige Alarmierung der Angreifenden

Üblicherweise wird vor der Bereinigung eines APT-Vorfalls der Angriff über längere Zeit hinweg beobachtet und forensisch analysiert, um so alle Zugangswege sowie die verwendeten Werkzeuge und Methoden zu identifizieren. Bemerken die Angreifenden während dieser Phase, dass sie entdeckt wurden, greifen sie eventuell zu Gegenmaßnahmen. Beispielsweise können sie versuchen, ihre Spuren zu verwischen, oder sie sabotieren noch weitere IT-Systeme. Auch könnten sie den Angriff zunächst abbrechen oder weitere Hintertüren einrichten, um den Angriff später fortzuführen.

Da bei einem APT-Angriff grundsätzlich davon ausgegangen werden muss, dass die gesamte IT-Infrastruktur der Institution kompromittiert wurde, ist das Risiko hoch, dass die Angreifenden die Bereinigungsaktivitäten entdecken. Das gilt insbesondere, wenn die kompromittierte IT-Infrastruktur benutzt wird, um die Bereinigung zu planen und zu koordinieren. Finden die wesentlichen Schritte zur Bereinigung nicht in der korrekten Reihenfolge statt oder werden kritische Maßnahmen nicht gleichzeitig und aufeinander abgestimmt durchgeführt, erhöht sich die Gefahr, dass die Angreifenden alarmiert werden. Isolieren die Zuständigen beispielsweise das Netz schrittweise statt auf einmal, werden die Angreifenden eventuell gewarnt, bevor ihr Zugriff effektiv beendet ist.

2.4. Datenverlust und Ausfall von IT-Systemen

Bei der Bereinigung eines APT-Vorfalls werden verschiedene IT-Systeme neu installiert und auch Netze temporär isoliert. Dadurch fallen zwangsweise IT-Systeme aus und Dienste sind damit z. B. nur noch eingeschränkt oder gar nicht mehr verfügbar. Dauert die Bereinigung sehr lange, kann dadurch die Produktivität der Institution ausfallen. Das kann wiederum signifikante wirtschaftliche Einbußen zur Folge haben, die sogar existenzbedrohend sein können. Dies ist insbesondere dann der Fall, wenn keine oder keine ausreichende Dokumentation für einen Wiederaufbau verfügbar ist.

2.5. Fehlender Netzumbau nach einem APT-Angriff

Bei einem APT-Angriff erlangen die Angreifenden detaillierte Kenntnisse darüber, wie die Zielumgebung aufgebaut und konfiguriert ist. Zum Beispiel kennen sie die existierenden Netzsegmente, Namensschemata für IT-Systeme, Konten sowie eingesetzte Software und Services. Durch dieses Wissen können sich dieselben Angreifenden unter Umständen auch nach einer Bereinigung erneut Zugang zur Zielumgebung verschaffen. Sie können sich sehr gezielt, effizient und unauffällig innerhalb des Netzes bewegen und in kurzer Zeit erneut einen hohen Infektionsgrad erreichen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

DER.2.3.A1 Einrichtung eines Leitungsgremiums (B)

Um einen APT-Vorfall zu bereinigen, MUSS ein Leitungsgremium eingerichtet werden, das alle notwendigen Aktivitäten plant, koordiniert und überwacht. Dem Gremium MÜSSEN alle für die Aufgaben erforderlichen Weisungsbefugnisse übertragen werden.

Wenn ein solches Leitungsgremium zu dem Zeitpunkt, als der APT-Vorfall detektiert und klassifiziert wurde, bereits eingerichtet ist, SOLLTE dasselbe Gremium auch die Bereinigung planen und leiten. Wurden schon spezialisierte Forensikdienstleistende hinzugezogen, um den APT-Vorfall zu analysieren, SOLLTEN diese auch bei der Bereinigung des Vorfalls miteinbezogen werden.

Ist die IT zu stark kompromittiert, um weiter betrieben zu werden, oder sind die notwendigen Bereinigungsmaßnahmen sehr umfangreich, SOLLTE geprüft werden, ob ein Krisenstab eingerichtet werden soll. In diesem Fall MUSS das Leitungsgremium die Bereinigungsmaßnahmen überwachen. Das Leitungsgremium MUSS dann dem Krisenstab berichten.

DER.2.3.A2 Entscheidung für eine Bereinigungsstrategie (B)

Bevor ein APT-Vorfall tatsächlich bereinigt wird, MUSS das Leitungsgremium eine Bereinigungsstrategie festlegen. Dabei MUSS insbesondere entschieden werden, ob die Schadsoftware von kompromittierten IT-Systemen entfernt werden kann, ob IT-Systeme neu installiert werden müssen oder ob IT-Systeme inklusive der Hardware komplett ausgetauscht werden sollen. Weiterhin MUSS festgelegt werden, welche IT-Systeme bereinigt werden. Grundlage für diese Entscheidungen MÜSSEN die Ergebnisse einer zuvor durchgeführten forensischen Untersuchung sein.

Es SOLLTEN alle betroffenen IT-Systeme neu installiert werden. Danach MÜSSEN die Wiederanlaufpläne der Institution benutzt werden. Bevor jedoch Backups wieder eingespielt werden, MUSS durch forensische Untersuchungen sichergestellt sein, dass dadurch keine manipulierten Daten oder Programme auf das neu installierte IT-System übertragen werden.

Entscheidet sich eine Institution dagegen, alle IT-Systeme neu zu installieren, MUSS eine gezielte APT-Bereinigung umgesetzt werden. Um das Risiko übersehener Hintertüren zu minimieren, MÜSSEN nach der Bereinigung die IT-Systeme gezielt daraufhin überwacht werden, ob sie noch mit den Angreifenden kommunizieren.

DER.2.3.A3 Isolierung der betroffenen Netzabschnitte (B)

Die von einem APT-Vorfall betroffenen Netzabschnitte MÜSSEN vollständig isoliert werden (Cut-Off). Insbesondere MÜSSEN die betroffenen Netzabschnitte vom Internet getrennt werden. Um die Angreifenden effektiv auszusperren und zu verhindern, dass sie ihre Spuren verwischen oder noch weitere IT-Systeme sabotieren, MÜSSEN die Netzabschnitte auf einen Schlag isoliert werden.

Welche Netzabschnitte isoliert werden müssen, MUSS vorher durch eine forensische Analyse festgelegt werden. Es MÜSSEN dabei sämtliche betroffenen Abschnitte identifiziert werden. Kann das nicht sichergestellt werden, MÜSSEN alle verdächtigen sowie alle auch nur theoretisch infizierten Netzabschnitte isoliert werden.

Um Netzabschnitte effektiv isolieren zu können, MÜSSEN sämtliche lokalen Internetanschlüsse, z. B. zusätzliche DSL-Anschlüsse in einzelnen Subnetzen, möglichst vollständig erfasst und ebenfalls berücksichtigt werden.

DER.2.3.A4 Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln (B)

Alle Zugangsdaten MÜSSEN geändert werden, nachdem das Netz isoliert wurde. Weiterhin MÜSSEN auch zentral verwaltete Zugangsdaten zurückgesetzt werden, z. B. in Active-Directory-Umgebungen oder wenn das Lightweight Directory Access Protocol (LDAP) benutzt wurde.

Ist der zentrale Authentisierungsserver (Domaincontroller oder LDAP-Server) kompromittiert, MÜSSEN sämtliche dort vorhandenen Zugänge gesperrt und ihre Passwörter ausgetauscht werden. Dies MÜSSEN erfahrene Administrierende umsetzen, falls erforderlich, auch mithilfe interner oder externer Expertise aus dem Bereich Forensik.

Wurden TLS-Schlüssel oder eine interne Certification Authority (CA) durch den APT-Angriff kompromittiert, MÜSSEN entsprechende Schlüssel, Zertifikate und Infrastrukturen neu erzeugt und verteilt werden. Auch MÜSSEN die kompromittierten Schlüssel und Zertifikate zuverlässig gesperrt und zurückgerufen werden.

DER.2.3.A5 Schließen des initialen Einbruchswegs (B)

Wurde durch eine forensische Untersuchung herausgefunden, dass die Angreifenden durch eine technische Schwachstelle in das Netz der Institution eingedrungen sind, MUSS diese Schwachstelle geschlossen werden. Konnten die Angreifenden die IT-Systeme durch menschliche Fehlhandlungen kompromittieren, MÜSSEN organisatorische, personelle und technische Maßnahmen ergriffen werden, um ähnliche Vorfälle künftig zu verhindern.

DER.2.3.A6 Rückführung in den Produktivbetrieb (B)

Nachdem das Netz erfolgreich bereinigt wurde, MÜSSEN die IT-Systeme geordnet in den Produktivbetrieb zurückgeführt werden. Dabei MÜSSEN sämtliche zuvor eingesetzten IT-Systeme und installierten Programme, mit denen der Angriff beobachtet und analysiert wurde, entweder entfernt oder aber in den Produktivbetrieb überführt werden. Dasselbe MUSS mit Kommunikations- und Kollaborationssystemen erfolgen, die für die Bereinigung angeschafft wurden. Beweismittel und ausgesonderte IT-Systeme MÜSSEN entweder sicher gelöscht bzw. vernichtet oder aber geeignet archiviert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.2.3.A7 Gezielte Systemhärtung (S)

Nach einem APT-Angriff SOLLTEN alle betroffenen IT-Systeme gehärtet werden. Grundlage hierfür SOLLTEN die Ergebnisse der forensischen Untersuchungen sein. Zusätzlich SOLLTE erneut geprüft werden, ob die betroffene Umgebung noch sicher ist.

Wenn möglich, SOLLTEN IT-Systeme bereits während der Bereinigung gehärtet werden. Maßnahmen, die sich nicht kurzfristig durchführen lassen, SOLLTEN in einen Maßnahmenplan aufgenommen und mittelfristig umgesetzt werden. Der oder die ISB SOLLTE den Plan aufzustellen und prüfen, ob er korrekt umgesetzt wurde.

DER.2.3.A8 Etablierung sicherer, unabhängiger Kommunikationskanäle (S)

Es SOLLTEN sichere Kommunikationskanäle für das Leitungsgremium und die mit der Bereinigung beauftragten Mitarbeitenden etabliert werden. Wird auf Kommunikationsdienste Dritter zurückgegriffen, SOLLTE auch hier darauf geachtet werden, dass ein sicherer Kommunikationskanal ausgewählt wird.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

DER.2.3.A9 Hardwaretausch betroffener IT-Systeme (H)

Es SOLLTE erwogen werden, nach einem APT-Vorfall die Hardware komplett auszutauschen. Auch wenn nach einer Bereinigung bei einzelnen IT-Systemen noch verdächtiges Verhalten beobachtet wird, SOLLTEN die betroffenen IT-Systeme ausgetauscht werden.

DER.2.3.A10 Umbauten zur Erschwerung eines erneuten Angriffs durch dieselben Angreifenden (H)

Damit dieselben Angreifenden nicht noch einmal einen APT-Angriff auf die IT-Systeme der Institution durchführen können, SOLLTE der interne Aufbau der Netzumgebung geändert werden. Außerdem SOLLTEN Mechanismen etabliert werden, mit denen sich wiederkehrende Angreifende schnell detektieren lassen.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende Dokumente zum Themenfeld APT veröffentlicht:

- Advanced Persistent Threats – Teil 4 Reaktion – Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung
- Common Criteria Protection Profile for Remote-Controlled Browsers Systems (ReCoBS): BSI-PP-0040

Das CERT-EU hat das weiterführende Dokument „CERT-EU Security Whitepaper 2014-007: Kerberos Golden Ticket Protection: Mitigating Pass-the-Ticket on Active Directory“ zum Themenfeld APT veröffentlicht.